KTB:ktb
AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Minnesota

UNITED STATES OF AMERICA

v.

STEVEN SCOTT BARTHOLOMAUS

FILED UNDER SEAL

Case No. 14mj1002 (SER)

CRIMINAL COMPLAINT

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief. On or about November 8, 2010, in Isanti County, in the State and District of Minnesota, defendant

> did knowingly distribute a visual depiction using a means and facility of interstate commerce and that had been mailed, shipped and transported in interstate commerce, by any means including by computer, where the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such depiction was of such conduct, to wit, a video file entitled "2010 Pthc 9yo Lizka Mast.mp4"

in violation of Title 18, United States Code, Sections 2252(a)(2) and (e).

I further state that I am a Special Agent and that this complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT OF MATTHEW VOGEL

Continued on the attached sheet and made a part hereof: ☒Yes ☐ No

Complainant's signature

Matthew Vogel, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 17 Nov. 2014

Judge's signature

City and state: St. Paul, Minnesota

The Honorable Steven E. Rau, U.S. Magistrate Judge
Printed name and title

 14mj1002(Starr)

STATE OF MINNESOTA)
) ss. AFFIDAVIT OF MATTHEW VOGEL
COUNTY OF RAMSEY)

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I. INTRODUCTION

I, Matthew Vogel, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent of the Federal Bureau of Investigation, and have been so employed since July, 2010. I am currently assigned to the Minneapolis Division, Squad C-3. My investigative responsibilities include investigation of cybercrime, child exploitation, and child pornography (hereinafter, CP), amongst other violations of Federal law. I have gained experience through training at the FBI Academy and everyday work relating to conducting these types of investigations. I have received training in the area of CP investigations and child exploitation, and have had the opportunity to observe and review numerous examples of CP (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also conducted searches pursuant to Federal search warrants relating to child exploitation and CP investigations.
2. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), and am empowered by 18 U.S.C. § 3052 to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.
3. I make this affidavit in support of a criminal complaint and arrest warrant. There is probable cause to believe that on November 8, 2010, Steven Scott Bartholomaus committed a violation of 18 U.S.C. §2252(a)(2), distribution of child pornography. Because this affidavit is submitted for the limited purpose of establishing probable cause to support the

contemporaneously filed application, it does not include each and every fact known to me or to other investigators.

4. The facts set forth in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement Agents, including foreign law enforcement agencies as described below; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by Federal Agents; independent investigation and analysis by FBI Agents/Analysts and computer forensic professionals; and my experience, training, and background as a Special Agent with the FBI.

5. The instant investigation, described more fully below, involves an Internet-based website hereafter referred to as "Website 10". The instant investigation has revealed that Steven Scott Bartholomaus was a registered member of "Website 10".

II. DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

The following definitions apply to this Affidavit:

6. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread" refers to a linked series of posts and reply messages. Message threads often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for

members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the bulletin board administrator.

7. "Child erotica," as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.

8. "Child Pornography," as used herein, is defined at 18 U.S.C. § 2256(8) as, "any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct".

9. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

10. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A DNS (domain name

system) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.fbi.gov, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

11. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

12. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

13. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

14. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming

code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

15. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

16. The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. "Internet Service Providers" (ISP), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a

computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

18. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

19. "Minor", as used herein, is defined at 18 U.S.C. § 2256(1) as, "any person under the age of eighteen years".

20. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

21. "Sexually explicit conduct", as used herein, is defined at 18 U.S.C. § 2256(2) as "actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person".

22. "Visual depictions", as used herein, is defined at 18 U.S.C. § 2256(5) as, "includ[ing] undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image.

23. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

III. PROBABLE CAUSE

Description of "Website 10"

24. "Website 10" was a CP website whose primary purpose was to advertise and distribute CP and discuss matters pertinent to the sexual abuse of children. On or about July 31, 2013, data from the computer server hosting "Website 10" was obtained from a web-hosting facility. Beginning on or about July 31, 2013, law enforcement Agents acting pursuant to an order of the United States District Court for the District of Maryland monitored electronic communications of users of "Website 10." Eventually, "Website 10" was seized by law enforcement agents. Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined, and documented the contents of "Website 10," which is described below.

25. "Website 10" had a message board whose primary purpose was the advertisement and distribution of CP and the discussion of matters pertinent to incest and pedophilia. Its name contains a reference to incest. The initial site web page contained the name of the site and an image depicting an adult male and female with a prepubescent female. The title in the image included the text, "Explaining sex to your little girl." According to statistics posted on the site, it contained 29,330 total posts, 3,800 topics and 10,397 members as of June 26, 2013.

26. Below the image on the main page of "Website 10" was a hyperlink to the site's discussion board. Accessing the hyperlink to the site's discussion board revealed a message board web page with the name of the site and the same image as described on the initial web page. Numerous forums and sub-forums were observed, including those entitled "Pics" and "Vids".

27. A review of the various topics within certain forums revealed, among other things, that a valid e-mail address was not required to register an account. However, a user would gain access to additional forums and topics by registering an account.

28. A review of the various topics within the other forums (such as "Pics" and "Vids") revealed, among other things, numerous image and/or video files that appeared to contain CP or child erotica. Each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included the post thread below it. Typical posts appeared to contain text, images, thumbnail previews of images, compressed files (such as ".rar" files), links to external sites, or replies to previous posts.

29. For example, the "Pics" forum also contained 10 additional sub-forums, some of which were titled "Girl Only Pics," "Bondage," and "Preteen." These forums all contained over 700

topics and over 5,000 posts. Further, each of these forums contained descriptions below the title; examples of which are as follows:

> Boys Only Pics: Post pics of just boys here. HC, SC, nude, whatever is OK.[1]
> Preschool: This area is for pics of ages 0-5.
> Preteen: This area is for pics of ages 6-12.

30. A review of topics within the aforementioned forums and sub-forums revealed numerous posts containing images depicting CP, bestiality, bondage, and child erotica of prepubescent children as young as toddlers; including those depicting anal, vaginal, or oral penetration. For example, on July 14, 2013, a user posted in the "Pics," "Preschool" sub-forum, a message containing the text "5yo" which contained 10 images depicting a partially naked prepubescent female wearing black stockings and black high-heel boots. Three of the images depicted the prepubescent female sitting on an object, bent forward, with her legs spread apart, exposing her anus and vagina. On December 21, 2012, a user posted a message in the "Pics," "Bondage" subforum that included three images depicting a naked early pubescent female with her wrists and ankles bound with rope. One of the images depicted the early pubescent female sitting in a chair with her legs spread apart, exposing her vagina. Her ankles and wrists are bound with rope and a green cylindrical object is penetrating her vagina. On June 10, 2012, a user posted a message in the "Pics," "Boy Only Pics" sub-forum that included two images depicting a naked prepubescent or early pubescent male and a naked adult male. One of the images depicted the adult male anally penetrating the prepubescent or early pubescent male.

---

[1] Based on my training and experience and information provided to me by others familiar with child exploitation investigations, I know that "HC" and "SC" are commonly used acronyms for "hard core" and "soft core" child pornography.

31. Upon registering for an account, numerous additional forums and sub-forums appeared on the main web page, including those entitled "PTCollector's Room" and "mature 4 young." A review of topics within these forums revealed they appeared to contain CP, child erotica, or text indicative of an interest in CP.

32. It was not required that a user log-into "Website 10" with a username and a password in order to access and download CP materials.

User "lolitalover" On "Website 10"

33. On September 17, 2011, the user "lolitalover" registered an account on "Website 10." That user included in the registration of the account, the email address stevebart2@hotmail.com. FBI agents conducting the investigation into "Website 10" noted this email address and conducted further investigation into its owner, as described below.

34. Between September 17, 2011, and September 18, 2011, "Website 10" user "lolitalover" initiated a bulletin board thread entitled "hello" where he posted the following message:

> "hello everyone, I'm Steve, I'm a middle aged man who just loves girls between the ages of 8-14, although of course, depending upon the girl!! Older and younger are okay too. I hope this board will stay around, thanks everyone, looking forward to meeting new friends with the same likes!"

35. "lolitalover" also sent/received 1 private message.

FBI Undercover Website: Background of Undercover Operation

36. The FBI's Innocent Images Operations Unit (IIOU) conducts undercover operations that target individuals with a predisposition to trafficking in CP. On or about March 16, 2009, a website, part of an undercover operation, became active on the Internet.

37. The FBI's undercover website is a web page that advertises access to free CP. The "home" page of the undercover website describes in detail that free CP will be available to view and

download once users enter in a password. The following is the advertisement on the home page:

> "Hello luvr of the forbidden and welcome to the real shock pornography. Spend a lot of time looking for real child pornography, but find only old trash? Then sincerely invite you into our world of forbidden CP!"
> "We share with you GBs of FREE forbidden porn video of children and preteen for your pleasure. All this video available for free download NOW! How do I access our site? Just enter your private password (if you have old password, make sure you get a new one), and your ready! If you like that then you will love this"
> "Theres more when you purchase VIP Account get access to Live Video and our database of over terabyte of CP. We are convinced this porn you have never seen!! All best series available, softcore and hard core CP pics and videos. New content of private yung and innocent added to VIP site often!"
> "Best of all VIP Account gives you LIVE VIDEO and sex chat with several beautiful child under your control. (hispeed internet necessary and 23 days needed for setup). This is real underage boys and girls performing private LIVE stream video only for you! Click here to learn how to get VIP Account."
> "We have servers in country with no laws against the beautiful child love. FBI and Interpol robot police cannot do anything against us! Even if we are shut down, we come up again in new location. We have been running since 2006!"

38. Individuals learn of the undercover website through a personal e-mail sent from the undercover Agent. Only individuals who have attempted to access or purchase CP through chat rooms, websites, newsgroups, or other online CP forums, receive these e-mail advertisements. The e-mail addresses of these individuals are obtained through other CP investigations. Recipients of the e-mail advertisements may delete the e-mail without accessing the website.

39. Individuals who receive this e-mail advertisement and want to access the webpage may do so in one of three ways. An individual may click on the hyperlink provided in the e-mail advertisement, or cut and paste the uniform resource locator (URL) into their web browser, or type the URL in their web browser.

40. Each recipient of the undercover advertisement e-mail is sent a unique password. Once an individual accesses the undercover home page, they have two options: they may close the website without attempting to download or access the free CP, or they may enter their unique password to gain entry and access to the second page of the website. Nothing on the website home page indicates any adult pornography or anything other than CP will be made available through this website.

41. After accessing the undercover website with their unique password, the individual is taken to the "second" page of the undercover website. The second page contains a list of approximately 25 CP videos available to view and/or download free of charge. Each video, described with a graphic title resembling that of a legitimate CP video, has a download "link" that purports to offer access to a free, one-minute sample.

42. In reality, when the user clicks on the download link, their web browser opens another webpage that appears to start the CP video download. Once the individual clicks the download link, their IP address, video sample number, the number of downloads attempted (including which videos were attempted) and other identifying information is recorded. However, no CP is ever actually made available to any individuals on the undercover website.

43. The undercover website also contains a "VIP ACCOUNT" link that an individual may click on. This is the area where individuals may, according to the home page text, pay for premium content and live streaming video of the sexual abuse of children per their personal direction. If an individual clicks on the "VIP ACCOUNT" link, they are redirected to the "VIP ACCOUNT page" of the undercover website. This page describes in further detail what is available after purchasing a VIP ACCOUNT. At the bottom of the "VIP

ACCOUNT" page there is a "Sign up for VIP ACCOUNT NOW!!" link that when clicked will redirect the user to the home page of the undercover Website. Users must again enter their unique password in order to return to the free download section of the undercover website. Each time an individual enters their unique password, their IP address is recorded.

44. On June 2, 2014, an FBI undercover Agent sent an e-mail to stevebart2@hotmail.com with an invitation to register for the undercover website. This email stated:

> "Nasty new site back up after tor crash!!! All girlz and boyzz under 12 and "family fun" [WEBSITE] use temp password [PASSWORD] to access all the yung ones you can handle."

45. On June 3, 2014 at 08:39:32 EDT, the undercover website recorded an individual using the Internet Protocol (IP) Address 75.161.134.196 used the unique password associated with the e-mail address stevebart2@hotmail.com and successfully logging into the undercover website. This user attempted to download 2 of the offered videos from the undercover website, as follows:

Video#:	Description:
116 (3 attempts)	Lolita Sasha1 Child Porn Pthc Pedo Kidsex Underage Reekiddymov Preteens Girls Children Preteen Fuck Kiddy Child Abus Sex Rape.avi
125	Hidden – Cam – Chubby black preteen giving head to white guy (PTHC) mpg

Evidence Related to Identification of User of "lolitalover" and "stevebart2@hotmail.com"

46. In October 2013, an administrative subpoena was issued to Microsoft in regards to the e-mail account stevebart2@hotmail.com.

47. A review of the results obtained on November 5, 2013 identified the user as Steve Bartholomaus of Minnesota, US.

48. Further, Microsoft provided the following IP address records as associated with the stevebart2@hotmail.com account: 67.4.139.214, 67.4.228.24, 67.4.157.223, 67.4.140.101,

67.4.225.72, and 67.4.134.114. A check of publicly available records revealed that those IP addresses were assigned to CenturyLink.

49. In December 2013, an administrative subpoena was issued to CenturyLink for the IP addresses 67.4.139.214, 67.4.228.24, 67.4.157.223, 67.4.140.101, 67.4.225.72, and 67.4.134.114.

50. A review of the results obtained on December 9, 2013 showed the IP address 67.4.139.214 on 9/5/2013 at 06:10 PT was assigned to subscriber Craig Bedbury, 35873 Polk St NE, Stanchfield, MN 55080.

51. A review of the results obtained on December 9, 2013 showed the IP address 67.4.228.24 on 7/17/2013 at 06:09 PT was assigned to MAYTAG Laundries, P.O. Box 127 Rush City, MN 55069.

52. A check of publicly available databases revealed Steven Bartholomaus, and Craig and Rebecca Bedbury reside at 35873 Polk St NE, Stanchfield, MN 55080. Minnesota Bureau of Criminal Apprehension records show Rebecca Bedbury is Bartholomaus' sister.

53. A Federal Search Warrant was issued on July 24, 2014 by the United States District Court for the District of Maryland, and was executed via e-mail to Microsoft Corporation for the e-mail address stevebart2@hotmail.com. A review of evidence gathered in the search revealed e-mails from May 26, 2006 through July 25, 2014. Between June 29, 2006 and July 2, 2006, there are several e-mail exchanges with the email address rick camburn <rickystarshine@hotmail.com> regarding the sale of David Hamilton photos on eBay. Based on the emails, Bartholomaus appears to have been selling photos, images, and movies by David Hamilton, who specializes in erotic nude photographs of young girls, early teens, and young women.

54. On June 23 and June 25, 2010, e-mails were sent to customerservice@acecashservices.com containing images of a paycheck for Steven S. Bartholomaus, 635 W. 5th St., Rush City, MN 55069. The check was from Rush City Bakery Inc., PO Box 213, Rush City, MN 55069.

55. On November 1, 2010 an e-mail was sent to goatfarmer@ireland.com with the subject "school girl pics". The body of the message included the following text "I saw your comment on imsgrc.ru, an I was wondering if i could see some of your pictures? I will sens some back if you let me know what kind you like."

56. On November 1, 2010, an email was sent to image@hushmail.com with the subject "imgsrc". The body of the message included the following text: "I was your posting on IMGSRC and I would love to chat with you about our mutual interest. Please contact me and let me know if you have msn or yahoo for chatting, or some other service you desire. Thank you!1 I love girls :)"

57. On November 8, 2010, an email was sent to ange-lys@hotmail.com with the subject "video,Ihope u get this". The body of the message included the following text: "This is a video of a beautiful young girl, having fun in front of the webcam :) I hope you like this". There was also an attached video titled "2010 Pthc 9yo Lizka Mast on Webcam.mp4". I viewed this video, and determined that it depicts a nude prepubescent female child masturbating and penetrating her genital area with her hand. The child's genital area is clearly visible in the video. The child depicted in this video has not yet been identified by law enforcement agents.

58. Based on my training and experience, I know that email messages travel via the Internet, which is a means of interstate commerce.

59. On March 10, 2013, an e-mail was sent to xinfo@immigration@gov.ph. The body of the message included the following text, "I arrived in the Philippines on March 8th, into the Manila airport, to visit my fiancee who lives in Cordova, Cebu...I have visited her 3 times previously with no problems, but this time I was excluded from entering the country..." and listed Bartholomaus' biographical information including passport number. A query of databases containing information on international travelers revealed that Bartholomaus has made several trips to Japan and the Phillippines. Bartholomaus travelled to Japan in 1998 and 2013, and to the Phillippines in 2007, 2008, and 2010.

60. A query of Minnesota Department of Driver and Vehicle Services databases revealed Bartholomaus renewed his driver license on September 3, 2014 and reported his address as 35873 Polk Street NE, Stanchfield, Minnesota.

61. On October 16, 2014 a physical surveillance of 35873 Polk St. NE, Stanchfield, Minnesota 55080, was conducted. The residence is described as a single story, single family dwelling with a sign on the right side of the driveway reading "35873 CRAIGS SHOP" (See Attachment A).

Steven Bartholomaus's Previous Child Pornography Conviction

62. In 1999, Bartholomaus pleaded guilty to one count receipt of child pornography in the United States Distrtict Court for the District of Minnesota, United States v. Bartholomaus, 99-cr-090 (MJD). This conviction around out of a 1998 United States Postal Inspection Service (USPIS) undercover investigation into receipt of CP via United States mail. USPIS conducted a controlled delivery of the tape requested by Bartholomaus and subsequently arrested Bartholomaus for violation of 18 U.S.C. 2252(a)(2). Bartholomaus was sentenced to

thirty-three months imprisonment and 3 years supervised release. Bartholomaus' requirement to register as a sex offender expired March, 2012.

VIII. CONCLUSION

63. I therefore submit that there exists probable cause to believe that on November 8, 2010, Steven Scott Bartholomaus violated 18 U.S.C. § 2252(a)(2), Distribution of Child Pornography.

RESPECTFULLY SUBMITTED

Matthew Vogel
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 17TH day of November, 2014

THE HONORABLE STEVEN E. RAU
UNITED STATES MAGISTRATE JUDGE